DESIGN PANEL NO. 43 12-16-97

RELIABLE MESSAGE THREAD ASSESSMENT - Steve Davis

OVERVIEW

This thread provides a substantial enhancement of the Reliable Message capability. This capability involves the reliable delivery of messages between end systems (Gateways, DDPs, CCPs, and CCWSs) within the RTPS.

Applications will utilize RM for exchanging messages over the RTCN and DCN. RM will provide reliability as follows:

- Messages will be re-transmitted upon detection of an unsuccessful delivery on either the RTCN or DCN.
- RM will utilize dual, redundant networks on the RTCN to ensure delivery in the event of a failure of a single network component.

RM will support both periodic (e.g., FD Change Data) and non-periodic (e.g., Commands, System Messages, etc.) message types. Delivery of RTCN periodic data will be done within the System Synchronous Rate (SSR) or the Display Synchronous Rate (DSR), as appropriate, including any re-transmissions.

In previous releases, RM was implemented as an API library, which was linked separately to each calling application. This resulted in non-deterministic performance, as there was no central, real-time control in executing the RM protocol.

For Atlas, RM will be implemented as a server process, with a companion API library for applications to access RM services. This will provide a central point of control for RM, and also streamline the manner in which events and errors are reported to Subsystem Integrity on each subsystem.

Results of discussion:

1. Thor requirements for recording will be accomplished with the Thor version of Reliable Messaging CSC.

2. The approach that is outlined in this presentation, and the schedule of milestones, will support the Atlas Development for recording DRP to SDC.

3. There is no requirement to support multiple activities on Gateway Subsystems. RM is required to support multiple activities on UNIX based RTPS subsystems.

4. Shawn Quinn will support the SE&I action for Performance Budget with respect to RM.

ACTIONS	ACTIONEE	DUE DATE	STATUS
No actions required			

DESIGN PANEL NO. 43 12-16-97

Approved

DESIGN PANEL NO. 43 12-16-97

ACCESS CONTROL AND SECURITY CSC - Tom Nguyen

OVERVIEW

The Access Control and Security (ACS) CSC provides access control and security policies for RTPS. ACS will be implemented over a series of CLCS deliveries and Thor will cover a minimal set of requirements. These policies will address user and system access, system file integrity, system security, and system auditing requirements. The boundaries of the ACS measurement are the network connection point of the individual system and it's internal configuration (i.e. Network traffic/data is not considered as part of this CSC). The ACS CSC are the software components that applies to each machine, and provides control and auditing capabilities using standard built-in COTS OS procedures and features.

Issues not addressed as a part of this panel

1. For Thor, recording only to Net Server (ACS Server).
2. SDC should record ACS data or not?
3. What is the overall concept for ACS ?
4. Keystroke recording capability? Requirement?
5. Recording over RON or DCN?

Access Control and Security Groundrules

The following is a list of groundrules and assumptions that relate to Access Control and Security CSC for Thor:

- The scope of ACS will be limited to RTPS.
- Security policies and guidelines are determined by SE&I.
- Firewall and network security including network monitoring, filtering, scanning, etc. is currently being implemented and will be re-evaluated in future deliveries for future requirements.
- ACS implementation will be provided by available built-in COTS software.
- ACS Gateway will not be implemented for Thor (TBD for future releases due to vendor OS).

DESIGN PANEL NO. 43 12-16-97

- Access Control and Security server shall have access to all RTPS platforms.
- ACS data will be in tape (4MM DAT) format.
- The central ACS data in not expected to exceed a maximum of 1GB of data per month to be transferred to tape (assuming a maximum of 50 hosts).

Results of discussion:

The Security Guidelines specifications for CLCS are being coordinated by Jeff Tysen as part of the overall CLCS security.

System Security will provide for the following:

1. CLCS Security Guidelines and procedures.

2. Define CLCS Security OPS Concepts.

3. Define additional SLS requirements.

4. Provide documents or update existing documents addressing 1,2, & 3 above.

This will be monitored as an ERP review.

ACTIONS	ACTIONEE	DUE DATE	STATUS

No actions required

Approved